# INHERENCY

Freedom Act masks reality of continuing surveillance

Solomon, Exec Dir Institute for Public Accuracy, 2015

[Normon, Executive Director Institute for Public Accuracy, veteran media critic, “Retooling the Patriot Act”, June 5-7, 2015, Counterpunch, <http://www.counterpunch.org/2015/06/05/retoolingthepatriotact/>

Some foes of mass surveillance have been celebrating the final passage of the USA Freedom Act, but Thomas Drake sounds decidedly glum. The new law, he tells me, is "a new spy program." It restarts some of the worst aspects of the Patriot Act and further codifies systematic violations of Fourth Amendment rights. In Oslo as part of a "Stand Up For Truth" tour, Drake warned at a public forum on Wednesday that "national security" has become "the new state religion." Meanwhile, his Twitter messages were calling the USA Freedom Act an "itty-bitty step" -- and a "stop/restart kabuki shell game" that "starts with restarting bulk collection of phone records." That downbeat appraisal of the USA Freedom Act should give pause to its celebrants. Drake is a former senior executive of the National Security Agency -- and a whistleblower who endured prosecution and faced decades in prison for daring to speak truthfully about NSA activities. He ran afoul of vindictive authorities because he refused to go along with the NSA's massive surveillance program after 9/11. Drake understands how the NSA operates from the highest strategic levels. He notes a telling fact that has gone virtually unacknowledged by anti-surveillance boosters of the USA Freedom Act: "NSA approved." So, of course, did the top purveyor of mendacious claims about the U.S. government's surveillance programs -- President Obama -- who eagerly signed the "USA Freedom" bill into law just hours after the Senate passed it. A comparable guardian of our rights, House Speaker John Boehner, crowed: "This legislation is critical to keeping Americans safe from terrorism and protecting their civil liberties." While some organizations with civil-liberties credentials have responded to the USA Freedom Act by popping open champagne bottles at various decibels, more sober assessments have also been heard. Just after senators approved the bill and sent it to the president, Demand Progress issued a statement pointing out: "The Senate just voted to reinstitute certain lapsed surveillance authorities -- and that means that USA Freedom actually made Americans less free." Another astute assessment came from CREDO, saying that Congress had just created "sweeping new authorities for the government to conduct unconstitutional mass surveillance of Americans." As it happened, the president signed the USA Freedom Act into law while four U.S. "national security" whistleblowers -- Drake as well as Coleen Rowley (FBI), Jesselyn Radack (Justice Department) and Daniel Ellsberg (Pentagon Papers) -- were partway through a "Stand Up For Truth" speaking tour from London to Oslo to Stockholm to Berlin. Traveling as part of the tour, I've been struck by the intensity of interest from audiences in the countries we've already visited -- Great Britain, Norway and Sweden -- where governments have moved to worsen repressive policies for mass surveillance. Right now, many people in Europe and elsewhere who care about civil liberties and want true press freedom are looking at the United States: to understand what an aroused citizenry might be able to accomplish, seeking to roll back a dangerous accumulation of power by an ostensibly democratic government. Let's not unwittingly deceive them -- or ourselves -- about how much ground the U.S. surveillance state has lost so far.

**Freedom Act sustains most Patriot Act surveillance**

Whitehead President of Rutherford Institute 2015

[John, President Rutherford Institute, “Free Speech, Facebook and the NSA: The Good the Bad the Ugly”, HuffPo, 4 June 2015 <http://www.huffingtonpost.com/john-w-whitehead/free-speech-facebook-and-_b_7497064.html>

Congress' legislative "fix," intended to mollify critics of the NSA, will ensure that the agency is not in any way hindered in its ability to keep spying on Americans' communications. The USA Freedom Act[could do more damage](http://www.washingtonpost.com/politics/senate-moves-ahead-with-retooling-of-us-surveillance-powers/2015/06/02/28f5e1ce-092d-11e5-a7ad-b430fc1d3f5c_story.html) than good by creating a false impression that Congress has taken steps to prevent the government from spying on the telephone calls of citizens, while in fact ensuring the NSA's ability to continue invading the privacy and security of Americans. For instance, the [USA Freedom Act](http://www.usatoday.com/story/news/politics/2015/06/02/patriot-act-usa-freedom-act-senate-vote/28345747/?csp=breakingnews) not only reauthorizes Section 215 of the Patriot Act for a period of time, but it also delegates to telecommunications companies the responsibility of carrying out phone surveillance on American citizens.  **And Now For The Downright Ugly News:** Nothing is going to change. As [journalist Conor Friedersdorf warns](http://www.theatlantic.com/politics/archive/2015/06/dont-underestimate-the-national-security-state/394571/), "Americans concerned by mass surveillance and the national security state's combination of power and secrecy should keep worrying."

Patel, co-director Liberty and Natl Security Program at Brennan Center, NYU Law School, 2015

Faiza Patel, The USA Freedom Act marks the beginning, not the end, of the fight to protect our privacy, June 25, 2015 http://america.aljazeera.com/opinions/2015/6/when-will-surveillance-reform-stop-being-just-cool.html#

We don’t know how many NSA databases of Americans’ information exist or how large they are. We do know that the Federal Bureau of Investigation dips into these archives of emails, texts, videos and chat messages with few constraints. In other words, information collected without any type of warrant or judicial review for intelligence purposes can be obtained by a U.S. law enforcement agency and used in a domestic criminal proceeding.

Freedom Act shows both parties support massive surveillance

Waldman, Sr. Writer at American Prospect, 2015

[Paul, “A reality check on the future of government spying,” Washington Post, 6/3/15]

It’s tempting to hail the passage yesterday of the subtly-named USA Freedom Act as a victory for civil liberties in America and a step toward a healthy recalibration of the government’s surveillance policies. But if that’s your feeling today, you might want to think twice. Not only are the changes the Freedom Act makes to existing practices relatively minor, both parties have signed on with the dramatic expansion of surveillance on law-abiding Americans that occurred after September 11. And both will continue to support it.

Freedom Act permits broad keyword surveillance; need more reform

Representative Polis 2015

[Jared, Republican from Colorado, original USA Freedom Act sponsor, A Victory for Privacy or Extension of Mass Surveillance? Co-Sponsor of USA FREEDOM Act Rejects Bill, *Democracy Now,* [http://www.democracynow.org/2015/6/4/a\_victory\_for\_privacy\_or\_extension#](http://www.democracynow.org/2015/6/4/a_victory_for_privacy_or_extension) ]

There was a blanket authorization, or at least the executive branch interpreted the authorization of the PATRIOT Act to provide them with the authority for a blanket authorization for metadata, etc., from people. That specific authority has been ended. Where the bill still goes too far, in my opinion, is it allows for keywords to be used for mass surveillance of information that’s retained at the phone companies. For instance, a city or geographical term, however specific—it might be the entire state of New York or California or Los Angeles, there’s really not any specific legal parameters around this—could still be used in a government request of information that continues to be stockpiled at a private company. We would also want to make sure that security concerns are addressed with regards to how companies maintain their databases of our personal information.

# SOLVENCY

SSRA warrants requirement strengthens Freedom Act

Attorney Ombres 2015

[Devon, “NSA domestic surveillance from the Patriot Act to the Freedom Act: The underlying history, constitutional basis, and the efforts at reform” Seton Hall Legislative Journal, Vol. 39(1): 27-58]

The FREEDOM Act is not without fault and could be strengthened by amending it to include some of the provisions of the piecemeal bills. For example, civil liberties advocates may feel that the FREEDOM Act does not strengthen minimization requirements to sufficiently address Judge Kollar-Kotelly’s ruling that PR and TT devices need not require specific identification of the target, thus permitting dragnet collection of metadata.138 This could be strengthened by including the portion of the SSR Act that requires a warrant for domestic surveillance.139

Surveillance State Repeal Act eliminates warrantless surveillance

Buttar 2015, Exec Dir Bill of Rights Defense Committee

[Shahid, “Can the Surveillance State Repeal Act Shift the Course on Spying?”, Apr 18, 2015http://www.occupy.com/article/can-surveillance-state-repeal-act-shift-course-spying]

Eager to reset the debate and anchor it in long overdue transparency, a bipartisan block of representatives have introduced a bill to restore civil liberties, privacy, and freedom of thought. The Surveillance State Repeal Act, HR 1466, would do this by repealing the twin pillars of the NSA dragnet: the PATRIOT Act (not only the three expiring provisions) and the 2008 FISA amendments. On multiple occasions, executive officials have lied under oath to congressional oversight committees about the scope of domestic surveillance. Yet the very same officials still appear in oversight hearings as if they maintained any credibility. It took whistleblowers resigning their careers to prove that senior government officials’ blithe assurances to Congress were in fact self-serving lies. Some members of Congress paid attention: the authors of the PATRIOT Act moved to curtail their own legislative opus, and have encouraged their colleagues not to reauthorize the expiring provisions unless they are first curtailed.

HR 1466 (the SSRA) represents a profound challenge by members of Congress from across the political spectrum fed up with the national security establishment and its continuing assault on our Constitution.

By repealing the twin pillars of the surveillance dragnet, the SSRA would essentially shift the burden of proof, forcing intelligence agencies like the NSA and FBI to justify the expansion of their powers from a constitutional baseline, rather then the illegitimate status quo.

Most policymakers forget the 9/11 commission’s most crucial finding: the intelligence community's failures that enabled the 9/11 attacks were not failures of limited data collection, but rather failures of data sharing and analysis.

Over the last 15 years, Congress has allowed the agencies to expand their collection capacities, solving an imaginary problem while creating a host of real threats to U.S. national security far worse than any act of rogue violence: the specter of state omniscience, immune from oversight and accountability, and thus vulnerable to politicization. This was among the fears of which President Eisenhower warned us in his last speech as President.

Meanwhile, the SSRA would preserve what the PATRIOT Act’s authors have said they meant to authorize: targeted investigations of particular people suspected by authorities to present potential threats.

HR 1466 would also advance transparency, both by protecting conscientious whistleblowers from the corrupt retaliation of agencies and careerists, and by giving judges on the secret FISA court access to technical expertise they have been denied.

Finally, the bill would directly address disturbing government duplicity, prohibiting agencies from hacking encryption hardware and software, and from using an executive order [12333] authorizing foreign surveillance as a basis to monitor Americans.

SSRA offers comprehensive surveillance reform

-strong protections make up for watered down Freedom Act

Clabough, Staff Writer New American, 2015

[Raven, “House Members Target Patriot Act with "Surveillance State Repeal Act,” 3-31-15. http://www.thenewamerican.com/usnews/constitution/item/20560-house-members-target-patriot-act-with-surveillance-state-repeal-act]

U.S. Representatives Mark Pocan (D-Wis., photo on left) and Thomas Massie (R-Ky.), who are seeking to repeal the PATRIOT Act in its entirety and combat any legal provisions that amount to American spying, unveiled their Surveillance State Repeal Act on Tuesday.

“This isn’t just tinkering around the edges,” Pocan said during a Capitol Hill briefing on the legislation. “This is a meaningful overhaul of the system, getting rid of essentially all parameters of the PATRIOT Act.”

“The PATRIOT Act contains many provisions that violate the Fourth Amendment and have led to a dramatic expansion of our domestic surveillance state,” added Massie (R-Ky.), who co-authored the legislation with Pocan. “Our Founding Fathers fought and died to stop the kind of warrantless spying and searches that the PATRIOT Act and the FISA Amendments Act authorize. It is long past time to repeal the PATRIOT Act and reassert the constitutional rights of all Americans.”

The House bill would completely repeal the PATRIOT Act, passed in the days following the 9/11 attacks, as well as the 2008 FISA Amendments Act, which permits the NSA to collect Internet communications — a program exposed by former NSA contractor-turned-whistleblower Edward Snowden. Likewise, the bill would reform the court that oversees the nation’s spying powers, enhance protections for whistleblowers, and stop the government from forcing technology companies to create easy access into their devices.

“The warrantless collection of millions of personal communications from innocent Americans is a direct violation of our constitutional right to privacy,” declared Congressman Pocan, adding, “Revelations about the NSA’s programs reveal the extraordinary extent to which the program has invaded Americans’ privacy. I reject the notion that we must sacrifice liberty for security. We can live in a secure nation which also upholds a strong commitment to civil liberties.” Massie stated, “Really, what we need are new whistleblower protections so that the next Edward Snowden doesn’t have to go to Russia or Hong Kong or whatever the case may be just for disclosing this."

According to The Hill, the bill is not likely to gain much traction, as leaders in Congress “have been worried that even much milder reforms to the nation’s spying laws would tragically handicap the nation’s ability to fight terrorists.”

A 2013 Surveillance State Repeal Act never picked up any momentum, and even bills with smaller ambitions have failed to gain passage. Senator Patrick Leahy (D-Vt.) introduced the USA Freedom Act in 2014, which sought to curtail the amount of mass surveillance that could be performed by the NSA and other groups.

As predicted, however, the bill was dramatically watered down during the consensus process. The White House signaled its “strong support” for the bill only after privacy protections and transparency provisions were substantially weakened.

Privacy advocates who once supported the USA Freedom Act were dismayed by its transformation into a consensus bill, which no longer prevented the NSA or FBI from warrantlessly sifting through international communications databases.

SSRA a comprehensive approach to curtailing warrantless surveillance

-prohibits dragnet surveillance, protects whistleblowers, bans exceptional acccess

Udry, Ex Dir Defending Dissent Foundation, June 2015

(Sue Udry (“Next Step After USA Freedom: Repeal The Surveillance State” http://www.defendingdissent.org/now/author/sue-udry/,June 17, 2015)

On June 1, the U.S. Senate allowed three provisions of the USA PATRIOT Act to expire. A few days later Congress enacted, and the President signed the USA Freedom Act, which introduced modest reforms to NSA mass surveillance. Everyone involved recognized that the bill was only a small reform. What’s next? What can Congress do to roll back unwarranted surveillance? The answer is the Surveillance State Repeal Act introduced by Representatives Mark Pocan (D-WI) and Thomas Massie (R-KY).

True to its name, the bill would repeal the two most notorious post-9/11 dragnet-surveillance laws and overhaul the National Security Agency’s domestic surveillance program. It’s an exceptionally strong and comprehensive bill supported by many civil-liberties organizations, including the Defending Dissent Foundation. In addition to repealing both the USA PATRIOT Act and the FISA Amendments Act, HR 1466 would reinstate a uniform standard requiring warrants based on probable cause for surveillance requests, and prohibit the federal government from forcing technology companies to build hardware or software “back doors” that allow its agencies to bypass encryption or privacy technology. The bill includes some legal protections for national-security whistleblowers, as well as changes to the Foreign Intelligence Surveillance Court to give it greater expertise in reviewing and challenging executive-branch applications for surveillance operations.

Strong SSRA provides robust protections

Udry, Ex Dir Defending Dissent Foundation, June 2015

(Sue Udry (“Next Step After USA Freedom: Repeal The Surveillance State” http://www.defendingdissent.org/now/author/sue-udry/,June 17, 2015)

“The warrantless collection of millions of personal communications from innocent Americans is a direct violation of our constitutional right to privacy,” Rep. Pocan said in a statement. “Revelations about the NSA’s programs reveal the extraordinary extent to which the program has invaded Americans’ privacy. I reject the notion that we must sacrifice liberty for security—we can live in a secure nation which also upholds a strong commitment to civil liberties. This [SSRA] legislation ends the NSA’s dragnet surveillance practices, while putting provisions in place to protect the privacy of American citizens through real and lasting change.” “The Patriot Act contains many provisions that violate the Fourth Amendment and have led to a dramatic expansion of our domestic surveillance state,” said Rep. Massie. “Our Founding Fathers fought and died to stop the kind of warrantless spying and searches that the Patriot Act and the FISA Amendments Act authorize. It is long past time to repeal the Patriot Act and reassert the constitutional rights of all Americans. I am proud to cosponsor Congressman Pocan’s bill and look forward to working with him on this issue.”

This bill was first introduced in 2013 by then-Rep. Rush Holt (D-NJ) who has since retired. The New York Times editorial board urged Congress to pass it primarily because of provisions prohibiting government “back doors” to bypass encryption. The Surveillance State Repeal Act, H.R. 1466, offers a complete repeal of the 2001 PATRIOT Act, which the NSA has cited as the legal basis for its phone metadata-harvesting surveillance program. It would also repeal the FISA Amendments Act, which contains provisions for email data-harvesting, while overhauling the NSA’s domestic surveillance program. Additionally, the bill would make retaliation against federal national-security whistleblowers illegal, and ensure that any FISA collection against a U.S. person takes place only pursuant to a valid warrant based on probable cause.

Richards, Wash University Law Prof, 2013

[Neil, The Dangers of Surveillance, 126 Harv. L. Rev. 1934 2012-2013, p. 1935]

At the level of theory, I will explain why and when surveillance is particularly dangerous and when it is not. First, surveillance is harmful because it can chill the exercise of our civil liberties. With respect to civil liberties, consider surveillance of people when they are thinking, reading, and communicating with others in order to make up their minds about political and social issues. Such intellectual surveillance is especially dangerous because it can cause people not to experiment with new, controversial, or deviant ideas. To protect our intellectual freedom to think without state oversight or interference, we need what I have elsewhere called "intellectual privacy."5 A second special harm that surveillance poses is its effect on the power dynamic between the watcher and the watched. This disparity creates the risk of a variety of harms, such as discrimination, coercion, and the threat of selective enforcement, where critics of the government can be prosecuted or blackmailed for wrongdoing unrelated to the purpose of the surveillance.

Richards, Wash University Law Prof, 2013

[Neil, Dangers of Surveillance, 126 Harv. L. Rev. 1934 2012-2013, p. 1940-1941]

It might seem curious to think of information gathering by private entities as "surveillance." Notions of surveillance have traditionally been concerned with the watchful gaze of government actors like police and prison officials rather than companies and individuals. But in a postmodern age of "liquid surveillance," the two phenomena are deeply intertwined. Government and nongovernment surveillance support each other in a complex manner that is often impossible to disentangle. At the outset, the technologies of surveillance - software, RFID chips, GPS trackers, cameras, and other cheap sensors -are being used almost interchangeably by government and nongovernment watchers.32 Private industry is also marketing new surveillance technologies to the state. Though it sounds perhaps like a plot from a paranoid science fiction novel, the *Guardian* reports that the Disney Corporation has been developing facial recognition technologies for its theme parks and selling the technology to the U.S. military. 33 Nor do the fruits of surveillance respect the public/private divide. Since the September II attacks, governments have been eager to acquire the massive consumer and Internet-activity databases that private businesses have compiled for security and other purposes, either by subpoena34 or outright purchase.35 Information can also flow in the other direction; the U.S. government recently admitted that it was giving information to insurance companies that it had collected from automated license-plate readers at border crossings.36 Similarly, while government regulation might be one way to limit or shape the growth of the data industry in socially beneficial ways, governments also have an interest in making privately collected data amenable to public-sector surveillance. In the United States, for example, the Communications Assistance for Law Enforcement Act of 199437 requires telecommunications providers to build their networks in ways that make government surveillance and interception of electronic communications possible.38 A European analogue, the EC Data Retention Directive Regulations of 2009, requires Internet service providers to retain details of all Internet access, email, and Internet telephony by users for twelve months, so that they can be made available to government investigators for cases of antiterrorism, intellectual property, child protection, or for other purposes.39 This surveillant symbiosis between companies and governments means that no analysis of surveillance can be strictly limited to just the government or the market in isolation. Surveillance must instead be understood in its aggregated and complex social context.

Richards, Wash University Law Prof, 2013

[Neil, Dangers of Surveillance, 126 Harv. L. Rev. 1934 2012-2013, p. 1947-1948]

Thus, in each of the traditional American justifications for freedom of speech,74 a commitment to freedom of thought - to intellectual freedom - rests at the core of the tradition. The second claim at the core of the theory of intellectual privacy is an empirical one - that surveillance inclines us to the mainstream and the boring. It is a claim that when we are watched while engaging in intellectual activities, broadly defined - thinking, reading, websurfing, or private communication - we are deterred from engaging in thoughts or deeds that others might find deviant. Surveillance thus menaces our society's foundational commitments to intellectual diversity and eccentric individuality. Richards, Wash University Law Prof, 2013

[Neil, Dangers of Surveillance, 126 Harv. L. Rev. 1934 2012-2013, p. 1948-1950]

Three different kinds of arguments highlight the ways in which surveillance can restrain intellectual activities. The first set of arguments relies on cultural and literary works exploring the idea that surveillance deters eccentric or deviant behavior. Many such works owe a debt to Jeremy Bentham's idea of the Panopticon, a prison designed around a central surveillance tower from which a warden could see into all of the cells. In the Panopticon, prisoners had to conform their activities to those desired by the prison staff because they had no idea when they were being watched. As Bentham describes this system, "[t]o be incessantly under the eyes of an Inspector is to lose in fact the power of doing ill, and almost the very wish.”75 Of course, the most famous cultural exploration of the conforming effects of surveillance is Orwell's harrowing depiction in *Nineteen Eighty-Four* of the totalitarian state personified by Big Brother.76 Orwell's fictional state sought to prohibit not just verbal dissent from the state but even the thinking of such ideas, an act punished as "thought-crime" and deterred by constant state surveillance. 77 Some scholars have documented how the modern surveillance environment differs from both the classic Panoptic on and a fully realized Big Brother in important ways.78 Nevertheless, Orwell's insight about the effects of surveillance on thought and behavior remains valid - the fear of being watched causes people to act and think differently from the way they might otherwise. Our cultural intuitions about the effects of surveillance are supported by a second set of arguments that comes from the empirical work of scholars in the interdisciplinary field of surveillance studies. Moving beyond the classic metaphors of the Panopticon and Big Brother, these scholars have tried to understand modern forms of surveillance by governments, companies, and individuals in all of their complexities. 79 The scope of this burgeoning literature has been wide-ranging and provides many examples of the normalizing effects of surveillance in a wide variety of contexts. In his pioneering work in the 1980s, for example, Professor Anthony Giddens argues that surveillance continually seeks the supervision of social actors and carries with it a permanent risk that supervision could lead to domination.80 More recent scholars have explored the risks that surveillance poses to democratic self-governance.81 One such risk is that of self-censorship, in terms of speech, action, or even belief. Studies of communist states give social-scientific accounts of many of the cultural intuitions about these self-censoring effects of surveillance,82 but so too do studies of modern forms of surveillance in democratic societies. For example, one study of the ED Data Retention Directive notes that "[u]nder pervasive surveillance, individuals are inclined to make choices that conform to mainstream expectations."83 As I explore below, the scope of surveillance studies is much broader than merely the study of panoptic state surveillance; scholars working in this field have examined the full scope of modern forms of watching, including data surveillance by private actors. But above all, surveillance scholars continually reaffirm that, while surveillance by government and others can have many purposes, a recurrent purpose of surveillance is to control behavior.84 A third and final set of arguments for intellectual privacy comes from First Amendment doctrine. A basic principle of free speech law as it has developed over the past century is that free speech is so important that its protection should err on the side of caution. Given the uncertainty of litigation, the Supreme Court has created a series of procedural devices to attempt to ensure that errors in the adjudication of free speech cases tend to allow unlawful speech rather than engage in mistaken censorship. These doctrines form what Professor Lee Bollinger calls the "First Pillar" of First Amendment law - the "[e]xtraordinary [p]rotection against [c]ensorship."85 Such doctrines take various forms, such as those of prior restraint, overbreadth, and vagueness, but they are often characterized under the idea of the "chilling effect." This idea maintains that rules that might deter potentially valuable expression should be treated with a high level of suspicion by courts. As the Supreme Court put it in perhaps its most important free speech decision of the twentieth century, *New York Times Co. v. Sullivan,86* the importance of uninhibited public debate means that, although "erroneous statement is inevitable in free debate, ... it must be protected if the freedoms of expression are to have the 'breathing space' that they 'need ... to survive. "'87

As Professor Frederick Schauer explains, "the chilling effect doctrine recognizes the fact that the legal system is imperfect and mandates the formulation of legal rules that reflect our preference for errors made in favor of free speech."88 Although the chilling-effect doctrine has been criticized on grounds that it overprotects free speech and makes empirically unsupported judgments,89 such criticisms miss the point. The doctrines encapsulated by the chilling effect reflect the substantive value judgment that First Amendment values are too important to require scrupulous proof to vindicate them, and that it is (constitutionally speaking) a better bargain to allow more speech, even if society must endure some of that speech's undesirable consequences. Intellectual-privacy theory explains why we should extend chilling-effect protections to intellectual surveillance, especially traditional-style surveillance by the state. If we care about the development of eccentric individuality and freedom of thought as First Amendment values, then we should be especially wary of surveillance of activities through which those aspects of the self are constructed.90 Professor Timothy Macklem argues that "[t]he isolating shield of privacy enables people to develop and exchange ideas, or to foster and share activities, that the presence or even awareness of other people might stifle. For better and for worse, then, privacy is sponsor and guardian to the creative and the subversive.91 A meaningful measure of intellectual privacy should be erected to shield these activities from the normalizing gaze of surveillance. This shield should be justified on the basis of our cultural intuitions and empirical insights about the normalizing effects of surveillance. But it must also be tempered by the chilling-effect doctrine's normative commitment to err on the side of First Amendment values even if proof is imperfect. Richards, Wash University Law Prof, 2013

[Neil, Dangers of Surveillance, 126 Harv. L. Rev. 1934 2012-2013, p. 1952-53]

The mechanics of intellectual privacy discussed so far depend upon knowing, or at least fearing, that someone might be watching us. If we have a sense of privacy, even one that turns out to be an illusion, we are less likely to change our behavior under the panoptic gaze. Truly secret and unexpected surveillance, from this perspective, might appear not to violate our intellectual privacy at all. If we have no inkling that we are being watched, if we really do not care that we are being watched, or if we fear no consequences of being watched, it could be argued that our intellectual freedom is unaffected. It can thus be argued that if the NSA Wiretapping Program had never leaked, it would have posed no threat to intellectual privacy. There are two problems with this account. First, no program of widespread surveillance is likely to remain secret forever. At some point, such a program will inevitably come to light, either by being leaked (as happened with the NSA program and the Army surveillance in *Laird),* or by actions taken pursuant to the program (such as prosecutions or disclosures). The injury suffered by those thus punished would serve as an example to the rest of us, and the mechanisms of intellectual privacy would come into effect at that point. Second, surveillance (even secret surveillance) can create additional harms that are separate from the ones suggested by intellectualprivacy theory. Scholars working in surveillance studies have explored the phenomenon of surveillance in all of its contemporary complexity, going beyond the Panopticon to consider private surveillance, the relationships between watchers and watched, and the wide variety of dangers that modern surveillance societies raise. 97 Recall in this regard that Lyon's definition of surveillance notes that surveillance has a purpose,98 but in the modern era this purpose is rarely totalitarian domination. All the same, most forms of surveillance seek some form of subtler influence or control over others. Even when surveillance is not Orwellian, it is usually about influencing or being able to respond to someone else's behavior. And while surveillance can sometimes have benign goals (like traffic safety, or parents using baby monitors or GPS trackers to keep tabs on their children), it is invariably tied to a particular purpose. Critically, the gathering of information affects the power dynamic between the watcher and the watched, giving the watcher greater power to influence or direct the subject of surveillance. 99 It might sound trite to say that "information is power," but the power of personal information lies at the heart of surveillance. The power effects of surveillance illustrate three additional dangers of surveillance: blackmail, discrimination, and persuasion. Vijayan, Correspondent, 2015

[Jaikumar, “For privacy advocates, USA Freedom doesn't end push for surveillance reform”, CS Monitor, June 3, 2015, http://www.csmonitor.com/layout/set/print/World/Passcode/2015/0603/For-privacy-advocates-USA-Freedom-doesn-t-end-push-for-surveillance-reform]

Several other groups including the American Civil Liberties Union, the Internet Infrastructure Coalition, and the Open Technology Institute expressed similar sentiments. “We’re celebrating because, however small, this bill marks a day that some said could never happen – a day when the NSA saw its surveillance power reduced by Congress,” the Electronic Frontier Foundation wrote. But most reform groups also noted that the Freedom Act leaves unchanged many other controversial surveillance practices. For instance, the Freedom Act does not change a FISA provision referred to as Section 702, which the government has used as its authority to conduct extensive surveillance on online communications. The government has cited Section 702 as its authority for programs like PRISM for collecting huge quantities of data directly from servers and networks belonging to several Internet giants including Google, Microsoft, Yahoo, and Facebook. The amount of records collected under Section 702 likely dwarfs the amount of records collected under the NSA's bulk phone records collection program Mr. Geiger said. Though Section 702 is meant to enable surveillance of terror suspects based outside the US, Mr. Geiger and [others](https://www.brennancenter.org/analysis/nsas-backdoor-search-loophole) say that in practice it enables warrantless backdoor collection of Internet communications belonging to many Americans. Sen. Ron Wyden (D) of Oregon is one of several lawmakers who have said they want additional reforms passed to rein in the "[dragnet surveillance](http://www.wyden.senate.gov/news/press-releases/wyden-statement-on-house-passage-of-usa-freedom-act)" enabled by Sec. 702. The provision is scheduled to sunset in 2017 and the effort has already begun to either kill it or reform it before renewal. Also unchanged by the Freedom Act are authorities granted to government under [Executive Order 12333](http://www.archives.gov/federal-register/codification/executive-order/12333.html) and statutes like the Electronic Communications Privacy Act (ECPA) of 1986. EO 12333 is a President Reagan era artifact that among other things assigns specific roles, responsibilities and rules for spying for more than a dozen intelligence agencies including the CIA, the NSA, and the FBI. Groups such as the Electronic Privacy Information Center have [cautioned](https://epic.org/privacy/surveillance/12333/) that the executive order often serves as an “alternate basis of authority for surveillance activities, above and beyond Section 215 and 702.” Activities such as the NSA's efforts to break online encryption and security technologies were likely conducted under the authority granted to the agency under the executive order. Vigo, filmmaker and human rights consultant, 2015

[Julian Vigo, “Bio-power and Security”, May 5, 2015 http://www.counterpunch.org/2015/05/05/biopowerandsecurity/]

Biopower is the bastard child of neoliberal societies which have created elaborate systems of surveillance to control the body in pursuit of securitizing culture. As we witnessed the involvement of medical, psychiatric and anthropological professionals during the last fourteen years of the United States’ War on Terror, the use of jurisprudence, medicine and social science has helped to create the body as political object, the body that necessitated being acted upon, being controlled, and even being locked away. The discourses of race and religion since 2001 quickly became conflated by various state apparati whereby the body as affect became part of the larger scope of racial, ethnic and religious profiling throughout the west. The barometer of tolerance was lowered and the biopolitical techniques used against the subject were excused in the name of the “greater good,” the securitization of the state and the protection of “our freedoms” against those who are, in the words of George W. Bush, “jealous of our freedoms.” The tautology is clear: “we” are an ideological threat to “them” because they covet our freedoms. This is a complete reversal of what is exercised in the War on Terror (i.e., “they” are a physical/security threat to “us”). Yet this Manichean terrain of freedom/terrorism and security/threat functions on a purely facile and blind acceptance of racial profiling, religious allegiances, and xenophobia. Never was it put into question what these freedoms are (or even if “they” actually exist) nor if these ostensible freedoms to disciplinary and regulatory power might actually have real effects on the lives of others. Very rarely did our media and juridic structures analyze the National Security EntryExit Registration System (NSEERS), also known as Special Registration, which focussed its surveillance on twenty-four predominantly Muslim nationalities requiring certain male noncitizens over the age of sixteen to register with Homeland Security. Everything down to the Muslim male body was renaturalized and repositioned in the bio-political theater where the recreated truth of the Muslim male was that of jealousy, danger, savagery, and inferiority. We have returned full circle to Edward Said’s orientalist analysis of Mohammadism, a purely western construct whose meaning had no resonance to Muslims. Fertilizer, a copy of the Qur’an, an accent, a video camera, or a prayer mat suddenly all became motives to search, sequester and detain, whilst the liberal citizens in whose name such racial profiling is carried out can be secured that indeed they are freer. The War on Terror evidences the most perverse and cynical of all possible self-fulfilling prophecies. The extralegal spaces created to control life—from myriad black sites, to Guantanamo Bay, to Abu Ghraib, to various prisons within the United States—all maintain the narrative of security, albeit unlawfully circumspect as arenas of political exception. The Muslim male body is made the surrogate for unlawful behavior, all in the name of security: his skin tone, his accent, his dress and manners, even when resembling that of the westerner, all render him immediately and always guilty. The suspension of the law in the name of “exception” has now become the norm and the body of the accused functions as a cultural synecdoche for the larger social body of Muslims. It is not at all surprising that the nude, duct taped body of John Walker Lindh, also known as “The American Taliban” or “Detainee 001″ in the War on Terror, became the object of a mediatized vivisection, the terrorist body laid bare to demonstrate that terror can come from within, even from a nice, “all-American” boy from California. Is it in the least shocking that John Walker Lindh did not take part in terrorist activities as he remains locked up in an Indiana prison for another seven years while the government which actually did aid the Taliban, United States, to the tune of at least $43 million has through the present day remained conspicuously uninvestigated? It is axiomatic that this War on Terror, almost in its fifteenth year, has nothing to do with investigating or stopping “terror.” Instead the Global War on Terror thrives upon constructing and disseminating innumerable fictions of perceived terrorist acts and terrorist bodies whilst abstracting a panorama of violence that will unceasingly be impossible to defeat both domestically and abroad. Ultimately, the War on Terror can never end. The nature of biopower in the context of state security today is twofold: first, to depersonify the object of western violence while humanizing the western pathos of the Global War on Terror; second, to recreate the enemy, reembodied and prepackaged as the Muslim “terrorist.” In this way, biopower functions to place focus on the body of the individual over the act, such as Foucault’s discussion of capital punishment which invokes less “the enormity of the crime itself than the monstrosity of the criminal…One had the right to kill those who represented a kind of biological danger to others” (1976, 138). Given the focus on the Muslim male body in contemporary western politics and the various behavioral typologies set up through the discourses of biopower today, it is not at all surprising that David Bruck is basing the defense of his client, Dzhokhar Tsarnaev, upon convincing the jury through photos of the “unrelenting punishment” of the ADX Supermax facility (known as a “clean version of hell”) while leaning heavily on western stereotypes of the Muslim male who, once executed, would necessarily become shahid (a martyr). In order for Tsarnaev to escape death, he must paradoxically be proven to be the stereotypical Muslim terrorist who will suffer more and achieve less fame in life than in death, rather than be shown as yet another angry man whose acts of murder might just speak to the larger issues of male violence the world over. Vigo, filmmaker and human rights consultant, 2015

[Julian Vigo, “Bio-power and Security”, May 5, 2015 http://www.counterpunch.org/2015/05/05/biopowerandsecurity/]

Reading Foucault’s conceptualization of the individual responsibility for herself requires the subject to adopt a posture of active engagement rather than one of passivity or of objectification in order to understand how “we constitute ourselves,” lending the active voice to traditionally passive manoeuvres in addressing power. This sort of challenge that Foucault offers, specifically his notion of critical ontology of ourselves, extends a Kantian critique of actualité within a philosophy that is neither concerned with telos nor origin, but one that is invested in locating the subject in the here and now. The ontology of ourselves, Foucault advocates, must disavow all projects that claim to be “global or radical,” adding: “In fact we know from experience that the claim to escape from the system of contemporary reality…has led to the return of the most dangerous traditions” (284). So while offering a voice to power, a maneuver that does not reify the subject at the very least, Foucault nonetheless acknowledges the problems of emancipatory narratives through which the subject can ostensibly liberate herself, while in fact such narratives, just like the homeomorphic surface of the Möbius strip, seemingly lead one back to the subject’s foundations of oppression.Freedom of the Press Foundation 2015

[Trevor Timm, Our Statement on Congress passing the USA Freedom Act, the NSA ‘Reform’ Bill, June 2, 2015, <https://freedom.press/blog/2015/06/ourstatementcongresspassingusafreedomactnsareformbill>

Today the Senate passed a version of the USA Freedom Act, a bill touted by its authors as surveillance reform that will end the NSA’s mass, suspicion-less collection of Americans’ personal data. Given that parts of the Patriot Act expired on June 1st, and that the government is pretending the expiration is a “crisis” rather than an opportunity, President Obama is expected to sign the bill as soon as possible. While the bill has many significant flaws, the USA Freedom Act vote is also historic: it’s the first time since the 1970s that Congress has indicated its intention to restrict the vast powers of intelligence agencies like the NSA, rather than exponentially expand them. It also shows the power that investigative journalism and brave whistleblowing can have on even the most entrenched government interests. Two years ago, debating these modest changes would’ve been unthinkable, and it is absolutely a vindication for Edward Snowden. Unfortunately, the bill is also woefully inadequate and largely symbolic, and Congress would’ve been better off letting Section 215 of the Patriot Act expire permanently. The USA Freedom Act supposedly bans bulk collection of phone records or any other private records, and we certainly hope it actually does. But its provisions are vague and confusing, leading many legal experts to believe they could be re-interpreted in secret—by NSA lawyers with a history of warping the common definitions of ordinary words beyond recognition—and could lead the FISA court to continue to allow the NSA to collect large quantities of Americans’ data in secret. (The administration will shamefully now re-start the phone program that expired on Monday for six months, as allowed under the new law's "transition" period.) The ultra-secret FISA court, a Kafkaesque nightmare for civil liberties, also gets to keep many of its worst features, with just minor changes around the edges. Such an anathema to democracy should be dismantled entirely. The USA Freedom Act also does not touch on two of the NSA’s most powerful and controversial tools: the FISA Amendments Act and Executive Order 12333, which have been used to scan untold billions of emails coming in and out of the United States, and give the agency free rein to spy on 95% of the world’s population with virtually no restrictions.  Vijayan, Correspondent, 2015

[Jaikumar, “For privacy advocates, USA Freedom doesn't end push for surveillance reform”, CS Monitor, June 3, 2015, http://www.csmonitor.com/layout/set/print/World/Passcode/2015/0603/For-privacy-advocates-USA-Freedom-doesn-t-end-push-for-surveillance-reform]

Supporters of surveillance reform took a brief moment on Tuesday to savor the Senate’s passage of the USA Freedom Act before immediately locking their sights on the next targets for change. The bill that was quickly signed into law by President Obama puts an end to the National Security Agency’s bulk collection of phone call metadata and imposes conditions and limits on how US spy agencies can use and access phone data. It also amends key portions of the Foreign Intelligence Surveillance Act of 1976 and the USA Patriot Act of 2005 with language that introduces greater transparency and oversight of government surveillance practices and the decisions of the FISA court. USA Freedom “is the most significant national surveillance reform in the last 30 years,” said Harley Geiger, advocacy director and senior counsel at the Center for Democracy and Technology. “It demonstrates that the era of rubber stamping mass surveillance is over.” Farivar, journalist and radio producer, 2015

[Cyrus Farivar, “Even former NSA chief thinks USA Freedom Act was a pointless change “And this is it after two years? Cool!”, Law & disorder / civilization & discontents, June 17, 2015 http://arstechnica.com/techpolicy/ 2015/06/evenformernsachiefthinksusafreedomactwasapointlesschange/ ]

The former director of the National Security Agency isn’t particularly concerned about the loss of the government’s bulk metadata collection under Section 215 of the Patriot Act. As Gen. Michael Hayden pointed out in an interview at a *Wall Street Journal* conference on Monday, the only change that has happened is that data has moved to being held by phone companies, and the government can get it under a court order. Hayden said: If somebody would come up to me and say,

“Look, Hayden, here’s the thing: This Snowden thing is going to be a nightmare for you guys for about two years. And when we get all done with it, what you’re going to be required to do is that little 215 program about American telephony metadata—and by the way, you can still have access to it, but you got to go to the court and get access to it from the companies, rather than keep it to yourself”—I go: “And this is it after two years? Cool!”

The NSA and the intelligence community as a whole still have many other technical and legal tools at their disposal, including the littleunderstood Executive Order 12333, among others. That document, known in government circles as "twelve triple three," gives incredible leeway to intelligence agencies sweeping up vast quantities of Americans' data. That data ranges from email content to Facebook messages, from Skype chats to practically anything that passes over the Internet on an incidental basis. In other words, EO 12333 protects the tangential collection of Americans' data even when Americans aren't specifically targeted—otherwise it would be forbidden under the Foreign Intelligence Surveillance Act (FISA) of 1978. Bill of Rights Committee/Defending Dissent Fndn, 2015

[“USA Freedom And The Surveillance State: The Debate is Only Just Beginning, June 2nd, 2015 https://www.popularresistance.org/usa-freedom-and-the-surveillance-state/]

The Bill of Rights Committee/Defending Dissent Foundation opposes the USA Freedom Act, and calls for a thorough congressional investigation into the surveillance authorities US intelligence agencies have claimed to gather the private information without a warrant of US persons who are not under suspicion of any crime. “Hundreds of thousands of Americans have joined the debate over unwarranted mass surveillance in the last two weeks, and over the last two years since the first Snowden revelation,” said Sue Udry, Executive Director of BORDC/DDF. “Massive trans-partisan civic participation has forced Congress for the first time to take action (albeit woefully inadequate) to rein in some unconstitutional spying.” Along with allies across the political spectrum, BORDC/DDF calls on Congress to use the expiration of Section 215 as a starting point for reforming the out of control surveillance practices of US intelligence agencies. Although the USA Freedom Act includes modest reforms, the FBI, NSA, and other intelligence agencies will be allowed to continue to collect private information about Americans who are under no suspicion of crime under Executive Order 12333 and the FISA Amendments Act. BORDC/DDF calls on Congress to pass the Surveillance State Repeal Act in order to bring surveillance programs in line with the Constitution. “We need a new Church Committee,” Udry said, referring to the Senate Select Committee to Study Governmental Operations that investigated intelligence operations in the 1970s and found significant wrongdoing. “Congress continues to operate in willful ignorance, refusing to demand a full accounting of all surveillance programs our intelligence agencies are using to gather information about innocent Americans. Without Snowden, neither Congress nor the people would have been aware of the NSA’s bulk data collection. What else is going on behind our backs?” Beyond the mass surveillance authorities in the bill, BORDC/DDF is concerned that transparency provisions are inadequate, and specifically exempt the FBI. This is particularly galling given a Department of Justice (DOJ) Inspector General report released two weeks ago that confirms the FBI has been using Section 215 to collect internet records in bulk , and violated the law regarding minimizing records for seven years. Further, the bill includes an increase to the maximum sentence for material support of terrorism, an unacceptably vague and expansive law that does not require a person to engage in or plan to engage in terrorism, or even knowingly support terrorism to be prosecuted. Since 9/11, the statute has become a favorite catch-all for the DOJ into which all sorts of constitutionally protected activities can be thrown and classified as suspect, if not criminal. Napolitano, Former Superior Ct New Jersey judge, 2015

[Andrew P., Lies the government is telling you: The ‘compromise’ USA Freedom Act fails to curtail NSA spying”, *Washington Times*, June 10, 2015]

Last week, Republicans and Democrats in Congress joined President Obama in congratulating themselves for taming the National Security Agency's voracious appetite for spying. By permitting one section of the Patriot Act to expire and by replacing it with the USA Freedom Act, the federal government is taking credit for taming beasts of its own creation. In reality, nothing substantial has changed. Under the Patriot Act, the NSA had access to and possessed digital versions of the content of all telephone conversations, emails and text messages sent between and among all people in America since 2009. Under the USA Freedom Act, it has the same. The USA Freedom Act changes slightly the mechanisms for acquiring this bulk data, but it does not change the amount or nature of the data the NSA acquires. Under the Patriot Act, the NSA installed its computers in every main switching station of every telecom carrier and Internet service provider in the United States. It did this by getting Congress to immunize the carriers and providers from liability for permitting the feds to snoop on their customers and by getting the Department of Justice to prosecute the only CEO of a carrier who had the courage to send the feds packing. In order to operate its computers at these facilities, the NSA placed its own computer analysts physically at those computers 24/7. It then went to the U.S. Foreign Intelligence Surveillance Act (FISA) Court and asked for search warrants directing the telecoms and Internet service providers to make available to it all the identifying metadata — the times, locations, durations, email addresses and telephone numbers used — for all callers and email users in a given ZIP code or area code or on a customer list. The first document revealed by Edward Snowden two years ago was a FISA court search warrant directed to Verizon ordering it to make available to NSA agents the metadata of all its customers — more than 113 million at the time. Once the court granted that search warrant and others like it, the NSA computers simply downloaded all that metadata and the digital recordings of content. Because the FISA court renewed every order it issued, this arrangement became permanent. Under the USA Freedom Act, the NSA computers remain at the carriers' and service providers' switching offices, but the NSA computer analysts return to theirs; and from there they operate remotely the same computers they were operating directly in the Patriot Act days. The NSA will continue to ask the FISA court for search warrants permitting the download of metadata, and that court will still grant those search warrants permitting the downloading. And the NSA will continue to take both metadata and content. The Supreme Court has ruled consistently that the government must obtain a search warrant in order to intercept any nonpublic communication. The Constitution requires probable cause as a precondition for a judge to issue a search warrant for any purpose, and the warrant must "particularly [describe] the place to be searched, and the persons or things to be seized." Because this is expressly set forth in the Constitution itself, Congress and the president are bound by it. They cannot change it. They cannot avoid or evade it. Probable cause is evidence about a person or place sufficient to permit a judge to conclude that evidence of a crime will probably be found. Both the Patriot Act and the USA Freedom Act disregard the "probable cause" standard and substitute instead a "government need" standard. This is, of course, no standard at all, as the NSA has claimed under the Patriot Act — and the FISA court bought the argument — that it needs all telephone calls, all emails and all text messages of all people in America. Today it may legally obtain them by making the same claim under the USA Freedom Act. When politicians tell you that the NSA needs a court order in order to listen to your phone calls or read your emails, they are talking about a FISA court order that is based on government need — not a constitutional court order, which can only be based on probable cause. This is an insidious and unconstitutional bait and switch. All this may start with the NSA, but it does not end there. Last week, we learned that the FBI is operating low-flying planes over 100 American cities to monitor folks on the streets and intercept their cellphone use — without any search warrants. Earlier this week, we learned that the Drug Enforcement Administration has intercepted the telephone calls of more than 11,000 people in three years — without any search warrants. We already know that local police have been using government surplus cell towers to intercept the cellphone signals of innocent automobile drivers for about a year — without search How dangerous this is. Amnesty International May 22 2014

**USA Freedom Act: Amnesty International is disappointed by the provisions of the bill designed to prohibit the bulk collection of data. An open list of “selectors” would be of concern since it does not allow individuals to foresee in what circumstances their communications might be intercepted. As such it may not fulfil the legality requirement. The open definition allows additions to the list of permitted types of specific selection term. The definition has also been expanded to include the terms “device” and “address”. This increases ambiguity and the scope for wide surveillance, as the terms could be interpreted as including devices and IP addresses that are used by large numbers of people rather than by a single individual. Amnesty International welcomes the recognition that surveillance must be targeted and may not be indiscriminate. At the same time we remain concerned that the bill may allow surveillance of millions of people and so it may not be strictly targeted. This also means that surveillance without probable cause is more likely. The bill should provide greater certainty by including a closed list of permitted types of "specific selection term" to make clear the extent to which mass surveillance is to be prohibited.**

**USA Freedom Act: The purpose for which data may be collected is too broad. It is not limited to terrorism, but only to “foreign intelligence information”. The U.S. government’s definition of “foreign intelligence information” includes “the conduct of foreign affairs”; it is so broad that it potentially encompasses the communications of almost any foreign person and in certain circumstances U.S. persons. This is unlikely to be necessary or proportionate. As set out above, second degree targeting and the use of an open list of “selection terms” means that it appears possible that mass surveillance may continue under the amended Act. In particular, the definition of "specific selection term"10 has been widened, meaning the protection it affords has been significantly weakened. The definition is now ambiguous and open to interpretation by the U.S. government, for example it is unclear whether the name of a state or a zip code might fall within it. If the government interprets the definition broadly, as its past record suggests is likely, this could allow surveillance on a large scale. As discussed above, we welcome the recognition that surveillance must be targeted and may not be indiscriminate. However remain concerned that the bill may allow surveillance of the communications of millions of people and thus may be neither necessary nor proportionate. The bill should include a closed list of permitted types of "specific selection term".**

Balkin, Yale Law Prof, 2008

Balkin, Jack M., "The Constitution in the National Surveillance State" (2008). Faculty Scholarship Series. Paper 225. http://digitalcommons.law.yale.edu/fss\_papers/225

Decades ago Michel Foucault argued that modern societies had become increasingly focused on watching and measuring people in order to control them, to normalize their behavior and to make them docile and obedient.51 His famous example was Jeremy Bentham’s idea of a Panopticon—a prison designed so that the prisoners could always be watched but would not know exactly when.52 By making surveillance ubiquitous, governments and private organizations could discourage behavior they deemed unusual or abnormal.

Today’s National Surveillance State goes beyond Foucault’s Panoptic model.

Government’s most important technique of control is no longer watching or threatening to watch. It is analyzing and drawing connections between data. Much public and private surveillance occurs without any knowledge that one is watched. More to the point, data mining technologies allow the state and business enterprises to record perfectly innocent behavior that no one is particularly ashamed of and draw surprisingly powerful inferences about people’s behavior, beliefs, and attitudes.53 Over time, these tools will only become more effective. We leave traces of ourselves continually, including our location, our communications contacts, our consumption choices—even our DNA.

Data mining allows inferences not only about the direct subjects of surveillance, but about *other people* with whom they live, work, and communicate.54 Instead of spying on a particular person, data about other persons combined with public facts about a person can allow governments and private businesses to draw increasingly powerful inferences about that person’s motives, desires, and behaviors.55

The problem today is not that fear of surveillance will lead people to docile conformity, but rather that even the most innocent and seemingly unimportant behaviors can increase knowledge about both ourselves and others.56 Normal behavior does not merely acquiesce to the state’s power; it may actually amplify it, adding information to databases that makes inferences more powerful and effective. Our behavior may tell things about us that we may not even know about ourselves. In addition, knowledge about some people can generate knowledge about others who are not being directly watched. Individuals can no longer protect themselves simply by preventing the government from watching them, for the government may no longer need to watch *them* to gain knowledge that can be used against them.

NSA surveillance essentially useless against terrorists

Bergen, et al, Dir. Natl Sec Prog @ New America Fnd, 2014

[Peter Bergen, David Sterman, Emily Schneider, and Bailey Cahall, Peter Bergen, director of the National Security Program @ New America Foundation. David Sterman and Emily Schneider are research assistants and Bailey Cahall is a research associate, National Security Program, New America Foundation, *Do NSA's Bulk Surveillance Programs Stop Terrorists?* January 2014 ]

However, our review of the government’s claims about the role that NSA “bulk” surveillance of phone and email communications records has had in keeping the United States safe from terrorism shows that these claims are overblown and even misleading.\* An in-depth analysis of 225 individuals recruited by al-Qaeda or a like-minded group or inspired by al-Qaeda’s ideology, and charged in the United States with an act of terrorism since 9/11, demonstrates that traditional investigative methods, such as the use of informants, tips from local communities, and targeted intelligence operations, provided the initial impetus for investigations in the majority of cases, while the contribution of NSA’s bulk surveillance programs to these cases was minimal. Indeed, the controversial bulk collection of American telephone metadata, which includes the telephone numbers that originate and receive calls, as well as the time and date of those calls but not their content, under Section 215 of the USA PATRIOT Act, appears to have played an identifiable role in, at most, 1.8 percent of these cases. NSA programs involving the surveillance of non-U.S. persons outside of the United States under Section 702 of the FISA Amendments Act played a role in 4.4 percent of the terrorism cases we examined, and NSA surveillance under an unidentified authority played a role in 1.3 percent of the cases we examined. Regular FISA warrants not issued in connection with Section 215 or Section 702, which are the traditional means for investigating foreign persons, were used in at least 48 (21 percent) of the cases we looked at, although it’s unclear whether these warrants played an initiating role or were used at a later point in the investigation.

Bergen, et al, Dir. Natl Sec Prog @ New America Fnd, 2014

[Peter Bergen, David Sterman, Emily Schneider, and Bailey Cahall, Peter Bergen, director of the National Security Program @ New America Foundation. David Sterman and Emily Schneider are research assistants and Bailey Cahall is a research associate, National Security Program, New America Foundation, *Do NSA's Bulk Surveillance Programs Stop Terrorists?* January 2014, p.2-3]

Finally, the overall problem for U.S. counterterrorism officials is not that they need vaster amounts of information from the bulk surveillance programs, but that they don’t sufficiently understand or widely share the information they already possess that was derived from conventional law enforcement and intelligence techniques. This was true for two of the 9/11 hijackers who were known to be in the United States before the attacks on New York and Washington, as well as with the case of Chicago resident David Coleman Headley, who helped plan the 2008 terrorist attacks in Mumbai, and it is the unfortunate pattern we have also seen in several other significant terrorism cases.

AT: “Successes are kept secret”

Bergen, et al, Dir. Natl Sec Prog @ New America Fnd, 2014

[Peter Bergen, David Sterman, Emily Schneider, and Bailey Cahall, Peter Bergen, director of the National Security Program @ New America Foundation. David Sterman and Emily Schneider are research assistants and Bailey Cahall is a research associate, National Security Program, New America Foundation, *Do NSA's Bulk Surveillance Programs Stop Terrorists?* January 2014, p4]

We acknowledge that the public record may not be complete and is evolving in a number of the cases we examined. As new information becomes available, we will update our assessment of the cases as merited. Additionally, there is reason to believe the government has at times actively concealed the role of NSA programs in investigations and criminal cases. Drug Enforcement Administration (DEA) agents have been trained in some instances, for example, to conceal the role of a DEA unit that analyzed metadata to initiate cases.8 Though this presents a challenge to our analysis, it seems unlikely that the government would conceal major cases of the NSA bulk surveillance programs’ purported successes at a time when it has to defend the programs’ very existence.

Bergen, et al, Dir. Natl Sec Prog @ New America Fnd, 2014

[Peter Bergen, David Sterman, Emily Schneider, and Bailey Cahall, Peter Bergen, director of the National Security Program @ New America Foundation. David Sterman and Emily Schneider are research assistants and Bailey Cahall is a research associate, National Security Program, New America Foundation, *Do NSA's Bulk Surveillance Programs Stop Terrorists?* January 2014, p4]

NSA surveillance of any kind, whether bulk or targeted of U.S. persons or foreigners, played an initiating role in only 7.5 percent of cases. To break that down further: The controversial bulk collection of telephone metadata appears to have played an identifiable role in, at most, 1.8 percent of the terrorism cases we examined. In a further 4.4 percent of the cases, NSA surveillance under Section 702 of targets reasonably believed to be outside of the country that were communicating with U.S. citizens or residents likely played a role, while NSA surveillance under an unknown authority likely played a role in 1.3 percent of the cases we examined.

Dissent News Wire, 2015

Exposing Repression, Reporting Resistance, Empowering Dissent. Update: Why USA Freedom Act Is Not A Win For Civil Liberties, But How What You Accomplished Can Help Change The Game, June 4, 2015 http://www.defendingdissent.org/now/news/updatewhyusafreedomactisnotawinforcivillibertiesbuthowwhatyouaccomplishedcanhelpchange...

There’s no evidence that these unconstitutional spying programs are making Americans safer. The Department of Justice’s Inspector General recently came out with a report saying that section 215 of the PATRIOT Act did not contribute in a meaningful way to a single national security related investigation. Not a single one! And what’s more, just before Memorial Day weekend a joint bulletin from the FBI, Department of Homeland Security and National Counterterrorism Center warned that intelligence analysts were overwhelmed with social media posts by Americans supporting ISIS. If our security agencies can’t even read all the social media posts by Americans raising their hands in support of terrorists, how can they make productive use of the telephone records of virtually every American?

# Adv 1: Clampdown- 2AC/1AR extensions

Surveillance crushes dissent

-Mass surveillance deters activism

Lerner, Constitutional Alliance spokesperson, 2014

(Mark, “The Chilling Effect of Domestic Spying” 8-5-14. http://americanpolicy.org/2014/08/05/the-chilling-effect-of-domestic-spying/)

The chilling effect can be simply defined as the way in which people alter or modify their behavior to conform to political and social norms as a result of knowing or believing they are being observed. The observation can be from physical surveillance, telephone meta data being collected, emails being intercepted and read, search engine requests being maintained, text messages being read and stored, financial transactions being monitored and much more. This paper will examine the chilling effect and provide some empirical data (links within this article) to show the chilling effect is real.

Denial is no longer an option. For years, even decades it has been reported by people inside and outside our government that agencies and departments within our federal government have been spying on citizens and further collecting data (Personal Identifiable Information) associated with the domestic spying taking place. Many of us who discussed the spying taking place were called conspiracy theorists, tin foil hat wearers, or black helicopter paranoid people: Today we are called realists.

The Snowden revelations are unique because of the depth and scope of the revelations and because Snowden had the official documents to back up his assertions. Previously people including former NSA analysts such as William Binney, Thomas Drake, Russell Tice and Kirk Wiebe had come forward asserting that our government was spying on citizens.

Too many in the government, the media, and the public dismissed the allegations of these men because it was “easy” to do so rather than believe the worst about our government, or actually having to do something about domestic spying. To be fair the NSA has not been the only ones accused of domestic spying. The FBI, DHS, and the CIA have also been proven to having done their own domestic spying; in the case of the FBI going back over seventy years. I support the need for our intelligence community, law enforcement, and our military. Unfortunately in much the same way the “Stockholm Syndrome” results in a person who has been kidnapped falling victim to the goals and aspirations of the kidnappers, the “rank and file” of those responsible for protecting us and our freedom have fallen victim to corrupt leadership in our intelligence and law enforcement communities. The culture of corruption is just as infectious as any chemical or biological weapon of mass destruction.

Congress has its share of the blame for the domestic spying that has and even to this day is taking place. After all it is congress that has the responsibility of oversight over agencies and departments of the federal government. All too often congress has failed to do what it has been tasked with doing; performing oversight. In fact, not too long ago congress gave retroactive immunity to telecom companies for the roles telecom companies played in illegally collecting information for the NSA at the request of former President Bush. When it comes down to it, there is plenty of “blame” to go around. Some are guilty: All are responsible including the public for not demanding better of our elected and appointed officials.

Whether a Democrat or Republican occupied the White House or regardless of which party controlled the Senate and/or the House of Representatives, domestic spying took place and is still taking place. Domestic spying is not a “Right” or “Left” issue. Domestic spying is an equal opportunity offender.Typically I would provide dozens of links in an article to substantiate what I am writing. In the case of the chilling effect I am only going to provide three links. The three links provide undeniable evidence that the chilling effect is real and how the chilling effect is affecting our country The bottom line is the chilling effect is not some psycho mumble jumble. The chilling effect is quantifiable based on empirical data. People were polled and research has been done. The public including lawmakers, young people, journalists and other “writers” have all too various degrees become subject to the chilling effect. Political scientists, attorneys, law professors, psychologists, sociologists have all weighed in on the chilling effect. I have read dozens of papers and other material accounting for thousands of pages about the “Chilling Effect”.

Depending on who is doing the research and the writing, it is fair and reasonable to assert that as much as 50% of people or more alter their behavior to conform to political and social norms as a direct result of the surveillance state that has been created in the United States. Up to 33% of journalists and other writers have admitted to changing what they write or say, or seriously considered changing what they write or say because they believe they are being “watched”.

What does all this mean to “activists” who are attempting to get the “general public” engaged in a whole host of issues from Common Core, Real ID, smart meters, immigration, national debt, healthcare, foreign policy and yes, even including domestic surveillance among other issues? What it means is the chilling effect will make it much more difficult to engage the general public much less educate and motivate the general public to “take a stand” and have their voices heard.

FBI surveillance predicated on racist stereotyping

Shamsi and others in 2014, Lecturer @ Columbia Law

(The Perversity of Profiling” – April 14th – available at the ACLU website - https://www.aclu.org/blog/perversity-profiling)

Using expanded authorities that permit investigations without actual evidence of wrongdoing, the FBI has also targeted minority communities for interviews based on race, ethnicity, national origin, and religion. It has used informants to conduct surveillance in community centers, mosques, and other public gathering places and against people exercising their First Amendment right to worship or to engage in political advocacy. And among America’s minority communities, “flying while brown” soon joined “driving while black” as a truism of government-sanctioned discrimination and stigma. It’s hard to overstate the damage done to the FBI’s relationship with minorities, particularly American Muslims. The damage, however, has spread further. When federal law enforcement leads in discriminatory profiling, state and local law enforcement will follow. Nowhere is that clearer than in New York City, where the NYPD – which is twice the size of the FBI – launched a massive program of discriminatory surveillance and investigation of American Muslims, mapping the places where they carry out daily activities and sending informants to spy on mosques and Muslim community organizations, student groups, and businesses. After the Associated Press broke a series of stories describing this program in stark and shocking detail, the NYPD defended itself, arguing that it was only doing what the FBI was permitted to do. Again, it’s hard to overstate the harm. From the ACLU’s work with New York’s Muslim communities, we know that a generation of youth is growing up fearful of its local police force, scared to exercise the rights to freedom of worship, speech, and association. Fortunately, the issuance of the revised Guidance on Race has been delayed and both the Justice Department and the civil rights community have a crucial opportunity to put a spotlight on the FBI, which vigorously opposes those fighting for equality. According to the New York Times, the FBI’s argument seems to be that it needs to identify where Somalis live to investigate potential Somali terrorism suspects. But that argument must be rejected for the same reason that we reject it in other contexts. Many mass shooters are young white males, yet we rightly don’t map where whites live or send informants to majority white communities to ferret out potential mass shooters. Put another way, the FBI’s argument presumes what the Ashcroft Guidance “emphatically rejects”: that crime can be prevented by the mass stereotyping of entire communities. Not only is that wrong, it is a ham-handed approach that squanders resources that should properly be devoted to investigating actual wrongdoing.

Surveillance deters political participation and activism

Electronic Frontier Foundation 2013

[EFF Files 22 Firsthand Accounts of How NSA Surveillance Chilled the Right to Association” 11-6-13. https://www.eff.org/press/releases/eff-files-22-firsthand-accounts-how-nsa-surveillance-chilled-right-association]

The Electronic Frontier Foundation (EFF) has provided a federal judge with testimony from 22 separate advocacy organizations detailing how the National Security Agency's (NSA) mass telephone records collection program has impeded the groups' work, discouraged their members and reduced the numbers of people seeking their help via hotlines. The declarations accompanied a motion for partial summary judgment filed late Wednesday, in which EFF asks the court to declare the surveillance illegal on two levels—the law does not authorize the program, and the Constitution forbids it.

In First Unitarian Church of Los Angeles v. NSA, EFF represents a diverse array of environmentalists, gun-rights activists, religious groups, human-rights workers, drug-policy advocates and others that share one major commonality: they each depend on the First Amendment's guarantee of free association. EFF argues that if the government vacuums up the records of every phone call—who made the call, who received the call, when and how long the parties spoke—then people will be afraid to join or engage with organizations that may have dissenting views on political issues of the day. The US government acknowledged the existence of the telephone records collection program this summer, after whistleblower Edward Snowden leaked a copy of a Foreign Intelligence Surveillance Court order authorizing the mass collection of Verizon telephone records.

"The plaintiffs, like countless other associations across the country, have suffered real and concrete harm because they have lost the ability to assure their constituents that the fact of their telephone communications between them will be kept confidential from the federal government," EFF Senior Staff Attorney David Greene said. "This has caused constituents to reduce their calling. This is exactly the type of chilling effect on the freedom of association that the First Amendment forbids."

Mass surveillance creates the legal, technical, and policy infrastructure for “turn-key” tyranny

Paglen 2013, Artist- activist & Geog Ph.D. from Berkeley

(Trevor, “Turnkey Tyranny: Surveillance and the Terror State” 6-23-13. http://creativetimereports.org/2013/06/25/surveillance-and-the-construction-of-a-terror-state/?gllry=opn)

By exposing NSA programs like PRISM and Boundless Informant, Edward Snowden has revealed that we are not moving toward a surveillance state: we live in the heart of one. The 30-year-old whistleblower told The Guardian’s Glenn Greenwald that the NSA’s data collection created the possibility of a “turnkey tyranny,” whereby a malevolent future government could create an authoritarian state with the flick of a switch. The truth is actually worse. Within the context of current economic, political and environmental trends, the existence of a surveillance state doesn’t just create a theoretical possibility of tyranny with the turn of a key—it virtually guarantees it.

For more than a decade, we’ve seen the rise of what we might call a “Terror State,” of which the NSA’s surveillance capabilities represent just one part. Its rise occurs at a historical moment when state agencies and programs designed to enable social mobility, provide economic security and enhance civic life have been targeted for significant cuts. The last three decades, in fact, have seen serious and consistent attacks on social security, food assistance programs, unemployment benefits and education and health programs. As the social safety net has shrunk, the prison system has grown. The United States now imprisons its own citizens at a higher rate than any other country in the world.

While civic parts of the state have been in retreat, institutions of the Terror State have grown dramatically. In the name of an amorphous and never-ending “war on terror,” the Department of Homeland Security was created, while institutions such as the CIA, FBI and NSA, and darker parts of the military like the Joint Special Operations Command (JSOC) have expanded considerably in size and political influence. The world has become a battlefield—a stage for extralegal renditions, indefinite detentions without trial, drone assassination programs and cyberwarfare. We have entered an era of secret laws, classified interpretations of laws and the retroactive “legalization” of classified programs that were clearly illegal when they began. Funding for the secret parts of the state comes from a “black budget” hidden from Congress—not to mention the people—that now tops $100 billion annually. Finally, to ensure that only government-approved “leaks” appear in the media, the Terror State has waged an unprecedented war on whistleblowers, leakers and journalists. All of these state programs and capacities would have been considered aberrant only a short time ago. Now, they are the norm. Politicians claim that the Terror State is necessary to defend democratic institutions from the threat of terrorism. But there is a deep irony to this rhetoric. Terrorism does not pose, has never posed and never will pose an existential threat to the United States. Terrorists will never have the capacity to “take away our freedom.” Terrorist outfits have no armies with which to invade, and no means to impose martial law. They do not have their hands on supra-national power levers like the World Bank and the International Monetary Fund. They cannot force nations into brutal austerity programs and other forms of economic subjugation. But while terrorism cannot pose an existential threat to the United States, the institutions of a Terror State absolutely can. Indeed, their continued expansion poses a serious threat to principles of democracy and equality.

At its most spectacular, terrorism works by instilling so much fear in a society that the society begins to collapse on itself. The effects of persistent mass surveillance provide one example of such disintegration. Most obviously, surveillance represents a searing breach of personal privacy, as became clear when NSA analysts passed around phone-sex recordings of overseas troops and their stateside spouses. And while surveillance inhibits the exercise of civil liberties for all, it inevitably targets racial, religious and political minorities. Witness the Department of Homeland Security’s surveillance of Occupy activists, the NYPD’s monitoring of Muslim Americans, the FBI’s ruthless entrapment of young Muslim men and the use of anti-terror statutes against environmental activists. Moreover, mass surveillance also has a deep effect on culture, encouraging conformity to a narrow range of “acceptable” ideas by frightening people away from non-mainstream thought. If the government keeps a record of every library book you read, you might be disinclined to check out The Anarchist Cookbook today; tomorrow you might think twice before borrowing Lenin’s Imperialism. Looking past whatever threats may or may not exist from overseas terrorists, the next few decades will be decades of crisis. Left unchecked, systemic instability caused by growing economic inequality and impending environmental disaster will produce widespread insecurity. On the economic side, we are facing an increasingly acute crisis of capitalism and a growing disparity between the “haves” and “have-nots,” both nationally and globally. For several decades, the vast majority of economic gains have gone to the wealthiest segments of society, while the middle and working classes have seen incomes stagnate and decline. Paul Krugman has dubbed this phenomenon the “Great Divergence.” A few statistics are telling: between 1992 and 2007, the income of the 400 wealthiest people in the United States rose by 392 percent. Their tax rate fell by 37 percent. Since 1979, productivity has risen by more than 80 percent, but the median worker’s wage has only gone up by 10 percent. This is not an accident. The evisceration of the American middle and working class has everything to do with an all-out assault on unions; the rewriting of the laws governing bankruptcy, student loans, credit card debt, predatory lending and financial trading; and the transfer of public wealth to private hands through deregulation, privatization and reduced taxes on the wealthy. The Great Divergence is, to put it bluntly, the effect of a class war waged by the rich against the rest of society, and there are no signs of it letting up. All the while, we are on a collision course with nature. Mega-storms, tornadoes, wildfires, floods and erratic weather patterns are gradually becoming the rule rather than the exception. There are no signs of any serious efforts to reduce greenhouse emissions at levels anywhere near those required to avert the worst climate-change scenarios. According to the most robust climate models, global carbon emissions between now and mid-century must be kept below 565 gigatons to meet the Copenhagen Accord’s target of limiting global warming to a two-degree Celsius increase. Meanwhile, as Bill McKibben has noted, the world’s energy companies currently hold in reserve 2,795 gigatons of carbon, which they plan to release in the coming decades. Clearly, they have bet that world governments will fail to significantly regulate greenhouse emissions. The plan is to keep burning fossil fuels, no matter the environmental consequences. While right-wing politicians write off climate change as a global conspiracy among scientists, the Pentagon has identified it as a significant threat to national security. After a decade of studies and war games involving climate-change scenarios, the Department of Defense’s 2010 Quadrennial Review (the main public document outlining American military doctrine) explains that “climate-related changes are already being observed in every region of the world,” and that they “could have significant geopolitical impacts around the world, contributing to poverty, environmental degradation, and the further weakening of fragile governments. Climate change will contribute to food and water scarcity, will increase the spread of disease, and may spur or exacerbate mass migration.” Nationally and internationally, the effects of climate change will be felt unevenly. Whether it’s rising water levels or skyrocketing prices for foods due to irregular weather, the effects of a tumultuous climate will disproportionately impact society’s most precarious populations. Thus, the effects of climate change will exacerbate already existing trends toward greater economic inequality, leading to widespread humanitarian crises and social unrest. The coming decades will bring Occupy-like protests on ever-larger scales as high unemployment and economic strife, particularly among youth, becomes a “new normal.” Moreover, the effects of climate change will produce new populations of displaced people and refugees. Economic and environmental insecurity represent the future for vast swaths of the world’s population. One way or another, governments will be forced to respond. As future governments face these intensifying crises, the decline of the state’s civic capacities virtually guarantees that they will meet any unrest with the authoritarian levers of the Terror State. It won’t matter whether a “liberal” or “conservative” government is in place; faced with an immediate crisis, the state will use whatever means are available to end said crisis. When the most robust levers available are tools of mass surveillance and coercion, then those tools will be used. What’s more, laws like the National Defense Authorization Act, which provides for the indefinite detention of American citizens, indicate that military and intelligence programs originally crafted for combating overseas terrorists will be applied domestically. The larger, longer-term scandal of Snowden’s revelations is that, together with other political trends, the NSA’s programs do not merely provide the capacity for “turnkey tyranny”—they render any other future all but impossible.

Adv 2: Encryption-2AC/1AR extensions

Congressional momentum now toward CISA-surveillance bill

Craig 2015, East Coast Editor for InfoWorld

[Caroline, Hello, Congress? CISA has nothing to do with data protection, InfoWorld, July 17, 2015]

More info sharing, less encryption -- that seems to be the prevailing prescription among politicians for improving cyber security, as recent events underscore yet again that many elected officials understand little or nothing about technology. Their zeal for pushing wrongheaded solutions puts us all at greater risk. The disconnect between problem and solution is especially obvious in the case of the recent OPM (Office of Personnel Management) hack. After 1.1 million fingerprints and personal data for 21.5 million people were stolen, Congress' response was to try to attach an amendment to a defense bill that would expand the exchange of data between the government and the private sector. As Senate Majority Leader Mitch McConnell (R-Ky.) intoned, referring to initial revelations about the theft at the OPM, "There are now 4 million extra reasons for Congress to act quickly." Would you feel safer knowing that the same government that fails to institute even basic security procedures like two-factor authentication and encryption of social security numbers wants to hoover up all your communications and personal data? As security expert Jonathan Zdziarski tweeted at the time, if you have two-step authentication enabled on Twitter, "then your tweets are safer than the government's data on 4 million federal employees and contractors." Reason prevailed, and last month's maneuver was blocked, but now Senate Majority Whip John Cornyn (R-Texas) is determined to forge ahead before the August break with CISA (Cybersecurity Information Sharing Act). "These cyber security issues are enormously significant," McConnell told "Fox News Sunday" over the weekend. Got that right -- the problem is CISA, as InfoWorld's David Linthicum has said, "does not do what it claims (protect us from cyber attacks) but instead makes it easier for the government to spy on us electronically." Security experts sent the Senate Committee on Intelligence a letter that exposes the "info-sharing" bill as both unnecessary and dangerous, and Wired magazine gave the bill "An F for Security But an A+ for Spying." But it seems Congress is not to be denied. This is the same group whose members "most of whom can't secure their own websites, and some of whom don't even use email," says The Guardian's Trevor Timm. While the executive branch recently promised to move all its websites over to HTTPS within two years, "there's not even a hint that Congress is attempting to do the same," Timm writes. Perhaps they've been listening to too many rants by FBI Director James Comey, whose fearmongering on the subject of encryption is whipping many in Congress into a frenzy. Never mind that security experts -- people who actually know something about encryption - - have hit back repeatedly. Their arguments are likely to fall on fallow ground, given the lack of technical know-how in Congress. "I think people would be shocked to know how little people [in Congress] know about these things," a former longtime Senate staffer told Politico, noting that Congressional offices have access to a lot of constituents' personal information. Politico quoted several staffers saying Congress does little to protect itself from cyber attacks, despite being a juicy target for foreign intelligence agencies. "Few could remember any kind of IT security training, and if they did, it wasn't taken seriously." The Congressman who oversees appropriation for the Department of Homeland Security, Rep. John Carter (R-Texas), speaking last week at a hearing on cyber security, prefaced his screed about the dangers posed by encryption by saying, "I don't know anything about this stuff." (Don't believe me? Watch the video.) This same bunch of people demanded (and got) the head of OPM chief Katherine Archuleta. But perhaps those in glass houses (of Congress) shouldn't throw stones. Granted, OPM showed a shockingly lax approach to cyber security and had been warned about the risks of its outdated technology as early as 2007. But "some of the security issues at OPM fall on Congress' shoulders," ArsTechnica writes. "Until recently, federal agents carried out background investigations for OPM. Then Congress cut the budget for investigations, and they were outsourced to USIS, which ... was essentially a company made up of 'some OPM people who quit the agency and started up USIS on a shoestring.'" OPM is hardly the only one with security problems. The list of issues seems endless: An audit early last month criticized lax security at the Internal Revenue Service, the Nuclear Regulatory Commission, the Energy Department, the Securities and Exchange Commission, and the Department of Homeland Security. The DHS intrusion detection system, called EINSTEIN, failed to detect the OPM breaches until after millions of records had been copied and removed. IRS systems still allow users to set their passwords to "password." And the Navy is spending $30 million to stay on Windows XP. But too many politicians remained faithfully obsessed with ending encryption and expanding surveillance capabilities.

Exceptional access requirements massively proliferate security risks

\*\*2AC extension

Hal Abelson, Prof of Electrical Engineering and Computer Science at MIT and the lead author of the MIT Computer Science and Artificial Intelligence Laboratory technical report, *Keys Under Doormats*, July 6, 2015

Political and law enforcement leaders in the United States and the United Kingdom have called for Internet systems to be redesigned to ensure government access to information — even encrypted information. They argue that the growing use of encryption will neutralize their investigative capabilities. They propose that data storage and communications systems must be designed for exceptional access by law enforcement agencies. These proposals are unworkable in practice, raise enormous legal and ethical questions, and would undo progress on security at a time when Internet vulnerabilities are causing extreme economic harm. As computer scientists with extensive security and systems experience, we believe that law enforcement has failed to account for the risks inherent in exceptional access systems. Based on our considerable expertise in real-world applications, we know that such risks lurk in the technical details.

In this report we examine whether it is technically and operationally feasible to meet law enforcement’s call for exceptional access without causing large-scale security vulnerabilities. We take no issue here with law enforcement’s desire to execute lawful surveillance orders when they meet the requirements of human rights and the rule of law. Our strong recommendation is that anyone proposing regulations should first present concrete technical requirements, which industry, academics, and the public can analyze for technical weaknesses and for hidden costs. Many of us worked together in 1997 in response to a similar but narrower and better-defined proposal called the Clipper Chip [1]. The Clipper proposal sought to have all strong encryption systems retain a copy of keys necessary to decrypt information with a trusted third party who would turn over keys to law enforcement upon proper legal authorization. We found at that time that it was beyond the technical state of the art to build key escrow systems at scale. Governments kept pressing for key escrow, but Internet firms successfully resisted on the grounds of the enormous expense, the governance issues, and the risk. The Clipper Chip was eventually abandoned.

A much more narrow set of law enforcement access requirements have been imposed, but only on regulated telecommunications systems. Still, in a small but troubling number of cases, weakness related to these requirements have emerged and been exploited by state actors and others. Those problems would have been worse had key escrow been widely deployed. And if all information applications had had to be designed and certified for exceptional access, it is doubtful that companies like Facebook and Twitter would even exist. Another important lesson from the 1990’s is that the decline in surveillance capacity predicted by law enforcement 20 years ago did not happen. Indeed, in 1992, the FBI’s Advanced Telephony Unit warned that within three years Title III wiretaps would be useless: no more than 40% would be intelligible and that in the worst case all might be rendered useless [2]. The world did not “go dark.” On the contrary, law enforcement has much better and more effective surveillance capabilities now than it did then. The goal of this report is to similarly analyze the newly proposed requirement of exceptional access to communications in today’s more complex, global information infrastructure. We find that it would pose far more grave security risks, imperil innovation, and raise thorny issues for human rights and international relations. There are three general problems.

First, providing exceptional access to communications would force a U-turn from the best practices now being deployed to make the Internet more secure. These practices include forward secrecy — where decryption keys are deleted immediately after use, so that stealing the encryption key used by a communications server would not compromise earlier or later communications. A related technique, authenticated encryption, uses the same temporary key to guarantee confidentiality and to verify that the message has not been forged or tampered with.

Second, building in exceptional access would substantially increase system complexity. Security researchers inside and outside government agree that complexity is the enemy of security — every new feature can interact with others to create vulnerabilities. To achieve widespread exceptional access, new technology features would have to be deployed and tested with literally hundreds of thousands of developers all around the world. This is a far more complex environment than the electronic surveillance now deployed in telecommunications and Internet access services, which tend to use similar technologies and are more likely to have the resources to manage vulnerabilities that may arise from new features. Features to permit law enforcement exceptional access across a wide range of Internet and mobile computing applications could be particularly problematic because their typical use would be surreptitious — making security testing difficult and less effective.

Third, exceptional access would create concentrated targets that could attract bad actors. Security credentials that unlock the data would have to be retained by the platform provider, law enforcement agencies, or some other trusted third party. If law enforcement’s keys guaranteed access to everything, an attacker who gained access to these keys would enjoy the same privilege. Moreover, law enforcement’s stated need for rapid access to data would make it impractical to store keys offline or split keys among multiple keyholders, as security engineers would normally do with extremely high-value credentials. Recent attacks on the United States Government Office of Personnel Management (OPM) show how much harm can arise when many organizations rely on a single institution that itself has security vulnerabilities. In the case of OPM, numerous federal agencies lost sensitive data because OPM had insecure infrastructure. If service providers implement exceptional 2 access requirements incorrectly, the security of all of their users will be at risk. Our analysis applies not just to systems providing access to encrypted data but also to systems providing access directly to plaintext. For example, law enforcement has called for social networks to allow automated, rapid access to their data. A law enforcement backdoor into a social network is also a vulnerability open to attack and abuse. Indeed, Google’s database of surveillance targets was surveilled by Chinese agents who hacked into its systems, presumably for counterintelligence purposes [3]. The greatest impediment to exceptional access may be jurisdiction. Building in exceptional access would be risky enough even if only one law enforcement agency in the world had it. But this is not only a US issue. The UK government promises legislation this fall to compel communications service providers, including US-based corporations, to grant access to UK law enforcement agencies, and other countries would certainly follow suit. China has already intimated that it may require exceptional access. If a British-based developer deploys a messaging application used by citizens of China, must it provide exceptional access to Chinese law enforcement? Which countries have sufficient respect for the rule of law to participate in an international exceptional access framework? How would such determinations be made? How would timely approvals be given for the millions of new products with communications capabilities? And how would this new surveillance ecosystem be funded and supervised? The US and UK governments have fought long and hard to keep the governance of the Internet open, in the face of demands from authoritarian countries that it be brought under state control. Does not the push for exceptional access represent a breathtaking policy reversal? The need to grapple with these legal and policy concerns could move the Internet overnight from its current open and entrepreneurial model to becoming a highly regulated industry.

Encryption does not impede *specific* investigations:

Reaching a warrant makes encryption more possible

McCullough 2015 Washington Correspondent

[Declan, “The Feds Want a Back Door Into Your Computer. Again.” Reason, May 2015, http://reason.com/archives/2015/04/09/the-feds-want-a-back-door-into]

It's certainly true that widespread use of encryption makes it more difficult for the government to peruse locked devices or to perform bulk surveillance of millions or billions of conversations. But the second point is more of a problem for the NSA's vacuum cleaner than it is for domestic police agencies, which have no legal mandate for such broad electronic spying. If police are investigating a specific person, recent history has shown that encryption is not an insurmountable obstacle. When an alleged New Jersey mobster was using encryption, FBI agents obtained a court order to sneak into his office and implant a key logger to snatch his passphrase. Using a Tor hidden service didn't prevent alleged Silk Road founder Ross Ulbricht, better known as "Dread Pirate Roberts," from being convicted of drug trafficking and money laundering. (Police also found a way to access Ulbricht's laptop without triggering his encryption software.) Device makers could likely be compelled by court order to implant government malware on customers' devices, given sufficient probable cause or other reasons. Metadata analysis remains possible, and files stored in the cloud may not always be encrypted. Snowden's cache of classified documents has revealed surprisingly aggressive techniques by the government, including deliberately weakening encryption standards.

Adv 3: Free internet- 2AC/1AR extensions

NSA surveillance spawns global internet nationalization

Ray 2014, Security Analyst at 21CT

[Tim ray, The Balkanization of the Internet, http://www.21ct.com/blog/the-revolution-will-not-be-tweeted-the-balkanization-of-the-internet-part-2/]

While countries are struggling with their own versions of this scenario and with how to spin this frightening picture of the new Balkanized Internet, they were handed a great gift: Edward Snowden’s tales of NSA’s global surveillance operations.

Suddenly, there’s a common enemy: America. Globally adventurous, the Americans (it seems) are also watching everyone they can, sometimes without permission. Snowden’s revelations alone will not be enough to force through the kinds of national controls we’re talking about, but they are a great start, a unifying force.

Sound farfetched? Maybe. Are there other answers? Perhaps. Brazil is moving forward with nationalizing its email services as well as plans to store all data within the country’s borders. The idea there is the same as the example above: take essential services in-country in order to prevent the U.S. from spying on them and (as a side effect) control them too. These proposals seem to be receiving some popular support; many see it as akin to nationalizing their oil, or another resource. Taking local control of formerly global services is the beginning of Balkanization for countries that choose that path.

Surveillance hampers efforts to promote Free Internet

-US not seen as credible in calling for open internet

-repressive governments use surveillance to justify heavy internet regulation

Kehl et al 2014, Policy Analyst @ Open Tech Institute

(Danielle Kehl = Policy Analyst at New America’s Open Technology Institute (OTI). Kevin Bankston = OTI Policy Director at OTI; Robyn Greene = OTI Policy Counsel, “Surveillance Costs: The NSA’s Impact on the Economy, Internet Freedom & Cybersecurity” July 2014. https://www.newamerica.org/downloads/Surveilance\_Costs\_Final.pdf)

The effects of the NSA disclosures on the Internet Freedom agenda go beyond the realm of Internet governance. The loss of the United States as a model on Internet Freedom issues has made it harder for local civil society groups around the world—including the groups that the State Department’s Internet Freedom programs typically support203—to advocate for Internet Freedom within their own governments.204 The Committee to Protect Journalists, for example, reports that in Pakistan, “where freedom of expression is largely perceived as a Western notion, the Snowden revelations have had a damaging effect. The deeply polarized narrative has become starker as the corridors of power push back on attempts to curb government surveillance.”205 For some of these groups, in fact, even the appearance of collaboration with or support from the U.S. government can diminish credibility, making it harder for them to achieve local goals that align with U.S. foreign policy interests.206 The gap in trust is particularly significant for individuals and organizations that receive funding from the U.S. government for free expression activities or circumvention tools. Technology supported by or exported from the United States is, in some cases, inherently suspect due to the revelations about the NSA’s surveillance dragnet and the agency’s attempts to covertly influence product development. Moreover, revelations of what the NSA has been doing in the past decade are eroding the moral high ground that the United States has often relied upon when putting public pressure on authoritarian countries like China, Russia, and Iran to change their behavior. In 2014, Reporters Without Borders added the United States to its “Enemies of the Internet” list for the first time, explicitly linking the inclusion to NSA surveillance. “The main player in [the United States’] vast surveillance operation is the highly secretive National Security Agency (NSA) which, in the light of Snowden’s revelations, has come to symbolize the abuses by the world’s intelligence agencies,” noted the 2014 report.207 The damaged perception of the United Statesas a leader on Internet Freedom and its diminished ability to legitimately criticize other countries for censorship and surveillance opens the door for foreign leaders to justify—and even expand— their own efforts.209 For example, the Egyptian government recently announced plans to monitor social media for potential terrorist activity, prompting backlash from a number of advocates for free expression and privacy.210 When a spokesman for the Egyptian Interior Ministry, Abdel Fatah Uthman, appeared on television to explain the policy, one justification that he offered in response to privacy concerns was that “the US listens in to phone calls, and supervises anyone who could threaten its national security.”211 This type of rhetoric makes it difficult for the U.S. to effectively criticize such a policy. Similarly, India’s comparatively mild response to allegations of NSA surveillance have been seen by some critics “as a reflection of India’s own aspirations in the world of surveillance,” a further indication that U.S. spying may now make it easier for foreign governments to quietly defend their own behavior.212 It is even more difficult for the United States to credibly indict Chinese hackers for breaking into U.S. government and commercial targets without fear of retribution in light of the NSA revelations.213 These challenges reflect an overall decline in U.S. soft power on free expression issues.

Domestic surveillance undermines US reputation

Sinha 2105, Human Rights Watch and ACLU

[G. Alex Sinha, “Better Privacy Protections Key to US Foreign Policy Coherence” – Defense One – March 25th - http://www.defenseone.com/ideas/2015/03/better-privacy-protections-key-us-foreign-policy-coherence/108469/]

For all its interest in promoting human rights around the world, you’d think the United States would be more sensitive to the ways its own surveillance policies undermine those very rights. Over the last few years, U.S. officials say they have spent more than $125 million to advance Internet freedom, which the State Department describes as a “foreign policy priority.” The U.S. rightly links Internet freedom with the freedoms of expression, peaceful assembly, and association, as well as with the work of human rights defenders. It makes sense, therefore, that the U.S. also actively funds human rights defenders, and calls out other governments for mistreating them. Yet surveillance conducted by the U.S. government—some of it unconstitutional and contrary to international human rights law—compromises Internet freedom, undermines the rights the government seeks to promote, and directly harms human rights defenders.

Domestic surveillance damages leadership on the Free Internet

Sinha of the ACLU and others in 2014

[Human Rights Watch, *With liberty to monitor all: How large-scale us surveillance is harming journalism, law and American democracy*, https://www.hrw.org/report/2014/07/28/liberty-monitor-all/how-large-scale-us-surveillance-harming-journalism-law-and

The questions raised by surveillance are complex. The government has an obligation to protect national security, and in some cases, it is legitimate for government to restrict certain rights to that end. At the same time, international human rights and constitutional law set limits on the state’s authority to engage in activities like surveillance, which have the potential to undermine so many other rights. The current, large-scale, often indiscriminate US approach to surveillance carries enormous costs. It erodes global digital privacy and sets a terrible example for other countries like India, Pakistan, Ethiopia, and others that are in the process of expanding their surveillance capabilities. It also damages US credibility in advocating internationally for internet freedom, which the US has listed as an important foreign policy objective since at least 2010. As this report documents, US surveillance programs are also doing damage to some of the values the United States claims to hold most dear. These include freedoms of expression and association, press freedom, and the right to counsel, which are all protected by both international human rights law and the US Constitution.

World adopts Free Internet norms only when US acts

[Gross 2013, Former Coordinator for Intl Communication and Info Policy @ State Dept

“Walking the Talk: The Role of U.S. Leadership in the Wake of WCIT,” 1-17-13. http://www.bna.com/walking-the-talk-the-role-of-u-s-leadership-in-the-wake-of-wcit-by-david-a-gross/]

It is important to recognize that the internet's political and policy future will be shaped by American leadership—not just through traditional U.S. rhetoric about competition, private sector leadership, and “multi-stakeholder” decision-making, but by America's ability to “walk the talk” by showing unequivocally that the ideals we preach internationally are fully reflected in what we do at home. American policymakers recognize that what we do domestically is watched and analyzed with great care by much of the rest of the world. For example, before the WCIT negotiations began in Dubai, Congress unanimously passed resolutions on internet governance that stated that “the United States should continue to preserve and advance the multi-stakeholder governance model under which the Internet has thrived as well as resist the imposition of an International Telecommunication Union (ITU) mandated international settlement regime on the Internet.” Declaring, among other things, that “it is essential that the Internet remain stable, secure, and free from government control.”

Congress's Clear Message Was Heard This action was important not only because of the substance of Congress's statements, but also because the world understood just how extraordinary it is for our Congress to act with unanimity, especially in an era when Congress has immense difficulty reaching consensus on almost anything. At the end of WCIT, I heard from many foreign officials that they knew that the United States would not sign the revised treaty with its Internet-related provisions because Congress had sent a clear and unequivocal message that such an agreement was unacceptable to the American people.

Looking ahead, we must recognize the obvious—internet policy issues affect virtually everyone in the world, and U.S. leadership depends on the power of its forward looking arguments, not just the historical fact that the United States gave the world a transformational technology. Although establishing global internet policy will be long, complex and challenging, we are fortunate that we have a well-established road map to follow.

No Room for Hypocrisy. We can continue to lead the world toward greater prosperity and the socially transformational benefits long associated with the internet. But if we fail to match our words with action; if we insist that others avoid an approach that imposes regulations and laws that limit the internet's capacity to advance freedom, openness and creativity, micromanages markets, or limits competition and investment, but do otherwise at home, then the world will quickly recognize our hypocrisy.

Free Internet is the best and first real protection against civilizational collapse in history

Dr. Eagleman 2010, Baylor College of Medicine

[David, Neuroscientist at Baylor College of Medicine, “ Six ways the internet will save civilization,” Wired, 9 Nov 2010, <http://www.wired.co.uk/magazine/archive/2010/12/start/apocalypse-no>]

Many great civilisations have fallen, leaving nothing but cracked ruins and scattered genetics. Usually this results from: natural disasters, resource depletion, economic meltdown, disease, poor information flow and corruption. But we’re luckier than our predecessors because we command a technology that no one else possessed: a rapid communication network that finds its highest expression in the internet. I propose that there are six ways in which the net has vastly reduced the threat of societal collapse. Epidemics can be deflected by telepresence One of our more dire prospects for collapse is an infectious-disease epidemic. Viral and bacterial epidemics precipitated the fall of the Golden Age of Athens, the Roman Empire and most of the empires of the Native Americans. The internet can be our key to survival because the ability to work telepresently can inhibit microbial transmission by reducing human-to-human contact. In the face of an otherwise devastating epidemic, businesses can keep supply chains running with the maximum number of employees working from home. This can reduce host density below the tipping point required for an epidemic. If we are well prepared when an epidemic arrives, we can fluidly shift into a self-quarantined society in which microbes fail due to host scarcity. Whatever the social ills of isolation, they are worse for the microbes than for us. The internet will predict natural disasters We are witnessing the downfall of slow central control in the media: news stories are increasingly becoming user-generated nets of up-to-the-minute information. During the recent California wildfires, locals went to the TV stations to learn whether their neighbourhoods were in danger. But the news stations appeared most concerned with the fate of celebrity mansions, so Californians changed their tack: they uploaded geotagged mobile-phone pictures, updated Facebook statuses and tweeted. The balance tipped: the internet carried news about the fire more quickly and accurately than any news station could. In this grass-roots, decentralised scheme, there were embedded reporters on every block, and the news shockwave kept ahead of the fire. This head start could provide the extra hours that save us. If the Pompeiians had had the internet in 79AD, they could have easily marched 10km to safety, well ahead of the pyroclastic flow from Mount Vesuvius. If the Indian Ocean had the Pacific’s networked tsunami-warning system, South-East Asia would look quite different today. Discoveries are retained and shared Historically, critical information has required constant rediscovery. Collections of learning -- from the library at Alexandria to the entire Minoan civilisation -- have fallen to the bonfires of invaders or the wrecking ball of natural disaster. Knowledge is hard won but easily lost. And information that survives often does not spread. Consider smallpox inoculation: this was under way in India, China and Africa centuries before it made its way to Europe. By the time the idea reached North America, native civilisations who needed it had already collapsed. The net solved the problem. New discoveries catch on immediately; information spreads widely. In this way, societies can optimally ratchet up, using the latest bricks of knowledge in their fortification against risk. Tyranny is mitigated Censorship of ideas was a familiar spectre in the last century, with state-approved news outlets ruling the press, airwaves and copying machines in the USSR, Romania, Cuba, China, Iraq and elsewhere. In many cases, such as Lysenko’s agricultural despotism in the USSR, it directly contributed to the collapse of the nation. Historically, a more successful strategy has been to confront free speech with free speech -- and the internet allows this in a natural way. It democratises the flow of information by offering access to the newspapers of the world, the photographers of every nation, the bloggers of every political stripe. Some posts are full of doctoring and dishonesty whereas others strive for independence and impartiality -- but all are available to us to sift through. Given the attempts by some governments to build firewalls, it’s clear that this benefit of the net requires constant vigilance. Human capital is vastly increased Crowdsourcing brings people together to solve problems. Yet far fewer than one per cent of the world’s population is involved. We need expand human capital. Most of the world not have access to the education afforded a small minority. For every Albert Einstein, Yo-Yo Ma or Barack Obama who has educational opportunities, uncountable others do not. This squandering of talent translates into reduced economic output and a smaller pool of problem solvers. The net opens the gates education to anyone with a computer. A motivated teen anywhere on the planet can walk through the world’s knowledge -- from the webs of Wikipedia to the curriculum of MIT’s OpenCourseWare. The new human capital will serve us well when we confront existential threats we’ve never imagined before. Energy expenditure is reduced Societal collapse can often be understood in terms of an energy budget: when energy spend outweighs energy return, collapse ensues. This has taken the form of deforestation or soil erosion; currently, the worry involves fossil-fuel depletion. The internet addresses the energy problem with a natural ease. Consider the massive energy savings inherent in the shift from paper to electrons -- as seen in the transition from the post to email. Ecommerce reduces the need to drive long distances to purchase products. Delivery trucks are more eco-friendly than individuals driving around, not least because of tight packaging and optimisation algorithms for driving routes. Of course, there are energy costs to the banks of computers that underpin the internet -- but these costs are less than the wood, coal and oil that would be expended for the same quantity of information flow. The tangle of events that triggers societal collapse can be complex, and there are several threats the net does not address. But vast, networked communication can be an antidote to several of the most deadly diseases threatening civilisation. The next time your coworker laments internet addiction, the banality of tweeting or the decline of face-to-face conversation, you may want to suggest that the net may just be the technology that saves us.